AMENDMENTS TO THE CLAIMS

Please cancel claim 10 and amend claim 1 with the following amended version thereof, without acquiescence in the grounds of rejection and without prejudice to pursue the original claims at a later time by continuation application or otherwise.

This listing of claims will replace all prior versions, and listings, of claims in the application.

LISTING OF CLAIMS

1. (Currently amended) A **[[gaming]]** security device for use in a cashless **[[gaming]]** system wherein portable data devices may be used to conduct cashless transactions, comprising:

a data device reader adapted to receive and read portable data devices;

a **[[game]]** host device physically proximate to said data device reader, said host device comprising a host device processor; and

a security module interposed between said data device reader and said **[[game]]** host device processor and uniquely identified with said host device, said security module preventing **[[communication]]** completion of a transaction involving **[[between]]** said data device reader and said **[[game]]** host device processor unless said data device reader is successfully cross-authenticated **[[by]]** with said security module **[[upon one of said]]** when a portable data device **[[devices being received by]]** is presented to and read by said data device reader,

independent of any authentication of said portable data device by said data device reader.

2. (Currently amended) The **[[gaming]]** security device of claim 1, wherein said portable data devices comprise smart cards, and wherein said data device reader comprises a smart card reader.

Claims 3-5 (Canceled).

6. (Original) A security module for use in a gaming device, comprising:

a data device reader interface for connection to a data device reader;

a gaming device interface for connection to a game device processor; and

a processor interposed between said data device reader interface and said gaming device interface, said processor configured to prevent communication between said data device reader and said game device processor unless said data device reader is first authenticated.

Claims 7-10 (Canceled).

Please add the following new claims:

11. (New) The security device of claim 1, wherein said host device comprises an electronic gaming machine, and wherein said host device processor controls the electronic gaming machine.

12. (New) The security device of claim 1, wherein, in addition to cross-authentication between said data device reader and said security module, said data device reader performs a cross-authentication check with the portable data device when it is presented to and read by said data device reader, and prevents a transaction with the portable data device if the cross-authentication check fails.

13. (New) The security device of claim 12, wherein said data device reader further comprises an internal security access module, said internal security access module adapted to automatically perform cross-authentication between said portable data device and said data device reader, and to automatically perform cross-authentication between said data device reader and said security module.

14. (New) The security device of claim 13, wherein said security module is configured to perform periodic authentication of said data device reader after the successful cross-authentication between said data device reader with said security module, and to prevent further communication between said data device reader and said host device processor if the periodic authentication fails.

15. (New) The security device of claim 13, wherein said internal security access module is adapted to generate a first random number, encipher said first random number using a common key to generate a first enciphered random number, send said first enciphered random number to said security module, receive a second enciphered random number from said security module, decipher said second enciphered random number using said common key to generate a second random number, generate a session key from said first random number and said second random number, receive a third enciphered number from said security module, decipher said third enciphered number using said session key to generate an authentication test value, and verify that said authentication test value matches said second random number.

16. (New) The security module of claim 6, wherein said processor is configured to perform a cross-authentication check with said data device reader, and wherein said data device reader is configured to perform a separate cross-authentication check with a portable data device.

17. (New) The security module of claim 6, wherein said processor is configured to generate a first random number, encipher said first random number using a common key to generate a first enciphered random number, send said first enciphered random number to said data device reader, receive a second enciphered random number from said data device reader, decipher said second

enciphered random number using said common key to generate a second random number, generate a session key from said first random number and said second random number, receive a third enciphered number from said data device reader, decipher said third enciphered number using said session key to generate an authentication test value, and verify that said authentication test value matches said second random number.

18. (New) A method of authentication for use in a cashless system wherein portable data devices may be used to conduct cashless transactions, said method comprising:

reading a portable data device with a data device reader physically proximate to a host device, said host device comprising a host device processor;

performing a cross-authentication between a said data device reader and a security module uniquely identified with said host device when a portable data device is presented to and read by said data device reader; and

preventing completion of a transaction involving said data device reader and said host device processor unless said data device reader is successfully cross-authenticated with said security module, independent of any authentication of said portable data device by said data device reader.

19. (New) The method of claim 18, wherein said host device comprises an electronic gaming machine, and wherein said host device processor controls the electronic gaming machine.

20. (New) The method of claim 18, further comprising the step of cross-authenticating the portable data device with the data device reader.

21. (New) The method of claim 18, wherein said data device reader is configured to perform the following steps in connection with cross-authenticating said security module:

generating a first random number at said data device reader;

enciphering said first random number using a common key to generate a first enciphered random number;

sending said first enciphered random number to said security module;

receiving, at said data device reader, a second enciphered random number from said security module;

deciphering said second enciphered random number using said common key to generate a second random number;

generating, at said data device reader, a session key from said first random number and said second random number;

receiving a third enciphered number from said security module, said third enciphered number comprising said first random number having been enciphered by said security module using said session key;

deciphering, at said data device reader, said third enciphered number using said session key to generate a first authentication test value; and

verifying that said first authentication test value matches said first random number.

22. (New) The method of claim 21, wherein said security module is configured to perform the following steps in connection with cross-authenticating said data device reader:

generating a second random number at said security module;

enciphering said second random number using a common key to generate said second enciphered random number;

sending said second enciphered random number to said data device reader;

receiving said first enciphered random number from said data device reader;

deciphering said first enciphered random number using said common key to generate said first random number;

generating, at said security module, said session key from said first random number and said second random number;

receiving a fourth enciphered number from said data device reader, said fourth enciphered number comprising said second random number having been enciphered by said data device reader using said session key;

deciphering, at said security module, said fourth enciphered number using said session key to generate a second authentication test value; and

verifying that said second authentication test value matches said second random number